MEMORANDUM FOR THE RECORD

FROM: DIMITRIOS VASTAKIS, BRANCH CHIEF OF WHITE HOUSE COMPUTER NETWORK DEFENSE

SUBJECT: CYBER SECURITY PERSONNEL LEAVING OFFICE OF THE ADMINISTRATION AT AN ALARMING RATE

DATE: OCTOBER 17, 2019

(U//FOUO) In the wake of a major cyber security incident in late 2014, the Office of the Chief Information Security Officer (OCISO) was established to take on the responsibility of securing the Presidential Information Technology Community (PITC) network. Over the course of four years the team had significantly matured the security posture of PITC and no major compromise has occurred since this model was implemented.

(U//FOUO) Unfortunately it was decided that the OCISO division was to be absorbed by the Office of the Chief Information Officer (OCIO). This is a significant shift in the priorities of senior leadership where business operations and quality of service take precedence over securing the President's network. As a career cyber security professional, this is alarming. Also of concern is the metric leadership is leveraging to gauge success of the cybersecurity program. Measuring the success of your security staff by the frequency major compromises are identified versus the duration of time since the last compromise is absurd.

(U//FOUO) It is my express opinion that the remaining incumbent OCISO staff is systematically being targeted for removal from the Office of the Administration (OA) through various means, such as: revocation of incentives, reducing the scope of duties, reducing access to programs, revoking access to buildings, and revoking positions with strategic and tactical decision making authorities. In addition, habitually being hostile to incumbent OCISO staff has been a staple tactic for the new leadership. It has forced the majority of GS-14 and GS-15 OCISO staff to resign. It is for this very reason why I submitted my resignation today. It is why the remaining OCISO staff will continue to resign.

(U//FOUO) I have seen the planned organizational structure for the cybersecurity mission going forward. It essentially transfers the entire mission to the White House Communications Agency (WHCA). All key decision making roles and leadership positions will no longer by staffed by EOP individuals. To me, this is in direct conflict with the recommendations made by the OA Office of General Counsel (OA GC). The main concern of OA GC was the oversight of PRA data and records. Considering the level of network access and privileged capabilities that cybersecurity staff have, it is highly concerning that the entire cybersecurity apparatus is being handed over to non-PRA entities.

(U//FOUO) They say that history repeats itself. Unfortunately, given all of the changes I've seen in the past three months, I foresee the White House is posturing itself to be electronically compromised once again. Allowing for a large portion of institutional knowledge to concurrently walk right out the front door seems contrary to the best interests of the mission and the organization as a whole.